Hendry County Sheriff's Office

General Order 5.9

TITLE: Field Mobile Data Computer	**SHERIFF'S APPROVAL:** Digital
ORIGINATION DATE: August 5, 2018	**REVISION DATE:** May 8, 2019
RELATED REFERENCES: *Department of Justice Criminal Information Services Security Policy, §119 F.S., GO 5.7 Information Services, GO 5.8 Internet Terms and Conditions* **CFA:** *26.04M, 32.01*	
REVIEW FREQUENCY: 3 YEARS	**DATE OF NEXT REVIEW:** May 8, 2022

I. PURPOSE: The purpose of this order is to provide members with guidance to the proper use of the mobile data computer.

II. SCOPE: This order shall apply to all sheriff's office members.

III. POLICY: The Hendry County Sheriff's Office recognizes the useful application of portable electronic devices when conducting law enforcement related functions. Sheriff's office members are encouraged to utilize portable electronic devices to facilitate the mission of the Hendry County Sheriff's Office, consistent with this policy and all other applicable state and federal regulations. It is the policy of the Hendry County Sheriff's Office to provide procedures governing the use of agency-owned portable electronic devices.

IV. PROCEDURE:

A. Acceptable Use

1. The purpose of the mobile data computer is to enhance the user's ability in the field to obtain necessary information in a timely manner, reduce radio traffic, provide dispatch information and increase safety. Due to the substantial cost and liability associated with this device, distinct guidelines must be established concerning the operation of the unit.

2. The use of this device must be in support of law enforcement and associated information exchange in the form of dispatch, case report, email, NCIC/FCIC, NLETS, CJNET, DHSMV data and other applicable law enforcement resources. Internet access will be restricted and any attempt to circumvent this restriction will result in termination of the user account.

3. All communications and information accessible by this device should be for a law enforcement purpose only, but are subject to public records requests as defined by Florida Statute.

4. Any illegal or unauthorized activities concerning the retrieval of criminal justice and personally identifiable information such as warrant, criminal histories, NLETS, FCIC/NCIC, CJNET and

DHSMV data will result in account termination and may produce civil and/or criminal prosecution.

5. All users must read and sign the Mobile Data Computer Agreement and Acceptable Use Statement prior to being issued a unit.
6. Due to the sensitive nature of the data that will be available to the user, the following guidelines must be established:

    a. All users must adhere to the current Information Technology Unit (ITU) policy regarding network and application usage (see General Order 5.8: Internet Terms and Conditions).

    b. Outside agency information services and shared data resources are also governed by this Procedure. All access, use, and dissemination of criminal justice and personally identifiable information shall be in accordance with the current FBI CJIS Security Policy

    c. All applicable users must be certified to use FCIC through an appropriate FDLE course prior to receiving access to FCIC via the mobile data computer.

    d. Additional software must be coordinated with the help desk and loaded into the computer by Information Technology Unit (ITU) personnel.

    e. No software may be removed or copied from the computer except as directed by ITU.

    f. While in the vehicle, the unit must be securely mounted and locked in the docking station with the key removed for security.

    g. No information will be obtained for the personal gain of the user or acquaintance. Any such attempt will result in account removal and potential criminal prosecution.

B. Equipment

1. Mobile data computer users shall respect and handle the computer as a sensitive electronic device.

    a. Users shall store the computer in a dry area with nominal temperature, as indicated by the manufacturer, when the unit is not being used. The computer should never be stored in the trunk of the vehicle.

    b. No food or drink is permitted in a mobile data computer work area.

    c. No decals, stickers or Velcro shall be adhered to the unit.

    d. The computer should not be plugged in and charging for more than 12 hours.

    e. During time period of high heat temperatures, a computer should not be used or left on when the air conditioning is off in the vehicle.

    f. While in use, the computer shall be placed in a position where air can circulate around the unit.

    g. During periods of high heat temperatures, computers need time to adjust to the surrounding climate. For example, if the unit is stored in a vehicle without air conditioning for 15 minutes, it should sit in the air conditioning for at least 15 minutes prior to turning on.

h. All computers deployed on any vessel of the Marine Unit must be stored in a sealed pelican case while the vessel is in motion, must never come in contact with the water, and must never be left powered on while stored in the pelican case.

i. In the case of equipment equipped with touch screens, no hard utensils such as pens, styluses or other pointing devices may come in contact with the screen unless the pointing device is manufacturer supplied.

2. Any damage or problems shall be reported to ITU personnel as soon as possible, and if necessary, the computer should be sent in for repair.

3. Failure to properly maintain and operate the computer, or damage due to neglect or abuse will be reported to the Crash Review Board.

a. Any damaged or inoperative computer submitted for repair will be assessed for damage caused by neglect, misuse or abuse to the unit.

b. The user will be notified if neglect, misuse or abuse is the determined cause and advised to complete the necessary documentation in accordance with Policy/Procedure 200.16: Loss Control. The user will then provide ITU personnel with the case report number issued for the report.

4. No component of the computer may be used for any purpose other than its original intent and configuration. No settings within the computer may be altered in any way.

5. Units assigned to spare cars shall not be removed except by the Information Technology Unit (ITU) personnel.

6. Computers that remain in any car, unused, must be turned off and the computer screen closed in order to prevent sun damage to the screen.

7. Failure to comply with these terms can result in account termination and/or recall of the computer.

C. Theft

1. Any attempt to liberate a component of the mobile data computer from another user for the purpose of augmenting or replacing lost items is prohibited and will result in immediate account termination and computer recall.

D. Security

1. Security within the confines of the mobile data computers is the highest priority in the Sheriff's Office network. Any actions by a user that may compromise this security will cause account termination and equipment recall. Examples of security breaches are identified but not limited to the following:

a. Sharing your account with another person.

b. Using another users account.

c. Leaving your computer unattended and unsecured while operational under your account.

d. Releasing another user's account information.

e. Release of criminal justice and personally identifiable information such as FCIC/NCIC, NLETS, CJNET, DHSMV or other information to a non-certified person.

f. Any other misuse as defined by FDLE or the FBI CJIS Security Policy with regard to FCIC/NCIC, NLETS, CJNET, DHSMV and law enforcement resource access.

g. All data accessed by each account is logged by FDLE, DHSMV and Smartcop.

E. Indemnity

1. The user specifically agrees to indemnify the Sheriff's Office for any criminal or civil litigation that may arise from the misuse of the data obtained by the user. Any information accessed by the user, either legal or illegal, is at the sole discretion of the user and holds no warranty by the Sheriff or the employees of the Sheriff's Office.

F. Exception of Terms and Conditions

1. All terms and conditions as stated in this document are applicable to the Sheriff's Office and all subscribers. These terms and conditions reflect the entire agreement of the parties and supersede all prior oral or written agreements and understandings of the parties. These terms and conditions will be governed and interpreted in accordance with the laws of the State of Florida.

V. GLOSSARY

INTERNET – Worldwide Network established by the Department of Defense Advanced Research Projects Agency for the purpose of information interchange.

MOBILE DATA COMPUTER – Any laptop computer issued for the purpose of field reporting, data collection or any other field use.

Your electronic signature in Power DMS acknowledges you have read this policy and understand it.